# Algoritmo euclideo delle divisioni successive

## Cos'è un algoritmo?

Intuitivamente si dispone di un ***algoritmo*** per risolvere un problema se si ha un elenco finito di istruzioni tali che:

1) a partire dai dati iniziali le istruzioni sono applicabili in maniera rigorosamente *deterministica*, cioè in modo che ad ogni passo sia sempre possibile stabilire univocamente quale è l'istruzione che deve essere applicata al passo successivo;
2) si disponga di un criterio univoco per stabilire quando si è raggiunto uno *stato finale*, quando cioè il processo deve considerarsi terminato e il risultato, se esiste, è stato ottenuto. Uno stato finale deve sempre essere raggiungibile in un numero *finito* di passi.

Il termine deriva dal nome del matematico persiano **Al-Khwarizmi** (780 – 850 ca) in quanto egli fu uno dei primi a far riferimento esplicito al concetto di algoritmo nel suo "*Libro della matematica orientale*". Dalla definizione di algoritmo è possibile evincere le due proprietà fondamentali di un algoritmo

- ***finitezza***, ovvero la sequenza delle istruzioni di un algoritmo deve essere finita;
- ***effettività***, ovvero ogni algoritmo deve portare ad un risultato.

Un algoritmo deve inoltre essere ***non ambiguo***, cioè le sue istruzioni devono essere comprensibili a chiunque le voglia applicare.
Per le caratteristiche di *finitezza* e di *determinismo*, un algoritmo si presta a essere automatizzato, cioè ad essere eseguito da una macchina opportunamente progettata.
La *teoria della calcolabilità* nasce nella terza decade del nostro secolo con l'esigenza, nata nell'ambito degli studi di *logica*, di fornire un equivalente rigoroso del concetto intuitivo di algoritmo, e di indagare le possibilità e i limiti dei metodi effettivi.

## *Esempi di algoritmi*

Sono esempi di algoritmi:

- le regole delle quattro operazioni matematiche;
- il metodo euclideo per il calcolo del massimo comun divisore;
- il metodo delle tavole di verità per stabilire se un'espressione logica è una tautologia.

## *Un altro esempio di algoritmo*

**Calcolare il *M.C.D. (massimo comun divisore)* di due numeri naturali diversi da zero**

1. Scomporre i numeri in fattori primi
2. Scegliere i fattori comuni
3. Scegliere quelli con esponente più piccolo
4. Moltiplicare tra loro i numeri scelti

*E. Modica*
www.galois.it

## Presentazione

Il matematico greco ***Euclide*** (323 a.C. – 285 a.C.) è stato il più importante studioso della storia antica. Egli è noto per i suoi ***Elementi***, un'importantissima opera costituita da 13 libri. Il matematico fu chiamato da Tolomeo I ad Alessandria d'Egitto per operare all'interno della più grande e famosa Biblioteca del mondo antico.
All'interno dei suoi *Elementi*, Euclide presenta due metodi per il calcolo del M.C.D. di due numeri. Uno di questi due metodi si basa sulle cosiddette "***divisioni successive***", grazie all'esistenza del seguente:

**Teorema (Elementi, VII libro)**. Siano $a, b \in \mathbb{N}$, con $a \geq b$ e $b \neq 0$. Esistono e sono unici due numeri naturali $q$, detto quoziente, e $r$, detto resto, tali che:

$$a = q \cdot b + r$$

e $0 \leq r < b$.

***Esempio***. Se si considerano i numeri 19 e 5, esistono e sono unici i numeri 3 e 4 tali che:

$$19 = 3 \cdot 5 + 4$$

## L'algoritmo delle divisioni successive

Se $r$ è il resto della divisione intera di due numeri $a, b \in \mathbb{N}$, con $a > b$, allora:
- se $r = 0$, si ha che $M.C.D.(a, b) = b$;
- se $r \neq 0$, si ha che $M.C.D.(a, b) = M.C.D.(b, r)$

Quindi, per trovare il $M.C.D.(a, b)$ basta eseguire le divisioni finché il resto non sarà uguale a zero.

***Esempio 1***. Determinare $M.C.D.(72,16)$.

$$72 : 16 = 4 \quad resto\ 8$$

Quindi $M.C.D.(72,16) = M.C.D.(16,8)$. Ma:

$$16 : 8 = 2 \quad resto\ 0$$

Quindi $M.C.D.(72,16) = 8$.

**Esercizi**. Calcolare il M.C.D. delle seguenti coppie di numeri.

a) 21, 49
b) 76,57
c) 240, 160
d) 80, 78
e) 78, 12
f) 98, 42
g) 102, 18
h) 468, 624

*E. Modica*
www.galois.it